Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Modernizing the E-rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	
	)	
	)	

To: The Commission

COMMENTS OF CISCO SYSTEMS, INC.

Jeffrey A. Campbell
Vice President, Government Affairs
Cisco Systems, Inc.
601 Pennsylvania Avenue, NW
Washington, DC 20003
(202) 354-2920

August 16, 2019

TABLE OF CONTENTS

I. Introduction and Summary 1
II. The Commission Should Extend the Category Two Budget Approach Permanently 2
III. The Eligible Services List Should Reflect Technology Changes in Internal Networks 3
A. Support Should Continue for Basic Maintenance of Schools' and Libraries' Internal Connections 3
B. The Definition of Internal Connections and Basic Maintenance Should Be Updated to Reflect Technology and Marketplace Changes 4
C. The Commission Should Recognize That Network Security Is a Critical Component of Internal Connections 5
IV. Equipment Transfer Rules Should Be Simplified to Reflect the Fixed Budget Approach 9
V. Conclusion 10

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Modernizing the E-rate Program for Schools and Libraries	)	WC Docket No. 13-184
	)	
	)	
	)	

To: The Commission

COMMENTS OF CISCO SYSTEMS, INC.

Cisco Systems, Inc. ("Cisco") submits these comments in response to the Commission's Notice of Proposed Rulemaking on making permanent the Category Two budget approach and other issues related to Category Two E-rate funding.[1]

I. INTRODUCTION AND SUMMARY

The five-year budget approach has proven to be a more effective way of allocating limited Category Two funding than the former two-in-five rule and should be adopted on a permanent basis. Consistent with the original intention, the five-year budgets should apply on a rolling basis to maximize schools' and libraries' flexibility to align their Category Two purchases with their internal connection needs.

The Commission also should take the opportunity of this proceeding to make other minor refinements to Category Two funding. In particular, in light of the spending discipline that the budgetary approach imposes, the Commission should (1) restore support for basic maintenance of internal connections; (2) update the rules to reflect technological and marketplace changes in

[1] *Modernizing the E-rate Program for Schools and Libraries,* Notice of Proposed Rulemaking, FCC 19-58 (rel. July 9, 2019) ("NPRM").

the way basic maintenance is supplied; and (3) recognize the critical importance of network security capabilities as a component of internal connections.

II. THE COMMISSION SHOULD EXTEND THE CATEGORY TWO BUDGET APPROACH PERMANENTLY

As revealed in the Bureau's 2018 Report, the five-year budget approach "resulted in a broader distribution of funding that is more equitable and more predictable for schools and libraries."[2] Specifically, as noted in the NPRM, the report found "four ways in which the category two budget approach appears to be more effective than the two-in-five rules approach" – (1) overall amount of funding disbursed, (2) broader participation and usage of Category Two support; (3) the distribution of Category Two funding is more like the distribution of E-rate support as a whole; and (4) greater flexibility to applicants to spend money effectively.[3] Cisco concurs in this assessment that the Category Two budgets approach has been much more effective at ensuring that schools and libraries have access to funding for internal connections that allows them to make use of Internet access service.

The Commission is therefore correct to propose to accept the Bureau's recommendation to make the five-year budget approach permanent. Cisco supports making the five-year budget approach permanent and eliminating the two-in-file rule.

Cisco has no position on whether schools' and libraries' five-year budget cycles should operate on a rolling basis or on a fixed cycle.[4] In planning for the transition, however, Cisco urges the Commission to recognize that, as the NPRM observes, the five-year Category Two

[2] NPRM at ¶ 3.

[3] *Category Two Budget Report* at ¶¶ 8-12.

[4] *See* NPRM at ¶¶ 32-33.

budgets have not been able to operate on a rolling basis because they were only adopted for the period from 2015-2019.[5] As a result, many applicants have operated under the reasonable assumption that they should plan their spending as if their five-year budgets would expire with the 2019 funding year. In light of this, the Commission should plan the transition to permanent five-year budget cycles so that all applicants have the opportunity for a budget "reset" starting with the 2020 funding year.

III. THE ELIGIBLE SERVICES LIST SHOULD REFLECT TECHNOLOGY CHANGES IN INTERNAL NETWORKS

A. Support Should Continue for Basic Maintenance of Schools' and Libraries' Internal Connections

As the Commission noted in 2014, E-rate stakeholders consistently have made clear "that basic maintenance is needed to ensure networks operate properly, particularly as networks become more complicated."[6] The only reason the Commission considered eliminating funding for basic maintenance was to address the inequitable distribution of Category Two funding—a concern that has been mooted by the five-year budget approach.[7] With the adoption of the fixed per-applicant budgets, it is now impossible for a few large school districts with high discount levels to monopolize the funding available for Category Two services. Given the demonstrated need for basic maintenance of internal connections and the new rule's effective control of the budgetary concern that prompted the proposal to eliminate basic maintenance, the Commission should adopt its proposal to continue funding for basic maintenance of internal connections.

---

[5] NPRM at ¶ 31.

[6] *2014 E-Rate Order* at 8918 ¶ 122.

[7] *Id.; see also* NPRM at ¶ 18.

B. The Definition of Internal Connections and Basic Maintenance Should Be Updated to Reflect Technology and Marketplace Changes

At the same time, the definition of "internal connections and basic maintenance" needs to be updated to reflect changing technology and support models. New cloud-based services and software technologies that are now the norm in education and have helped schools deliver better educational and professional development services to their students and staff. These systems are especially prevalent in schools with lean IT budgets, where funding is unavailable for staff to manage, monitor, and maintain traditional hardware solutions.

The shift toward the cloud-based services and software technologies, including Software-as-a-Service, software-defined networking, software subscriptions and licensing, means that schools are moving away from a traditional "break-fix" hardware technology environment. Solutions to customer problems now are provided in the cloud and in school networks themselves on a regular basis, allowing critical service support and security updates to occur without hardware changes. Basic maintenance is still necessary for hardware components, but it is being outstripped by the need for technology maintenance to both hardware and software—often delivered from the cloud.

Systems can be accessed, assessed, and fixed remotely. Software patches can be delivered automatically and remotely, reducing the amount of time to fix bugs, update and maintain systems, and ensure greater uptime. Threat attackers are constantly changing their techniques and tactics,often moving quickly to new technologies. School system administrators now require software support models to make sure not only that these systems are up and running, but that they can be safely operated in a dynamic threat environment.

In many cases, today's basic maintenance solutions for internal networks are provided via enterprise agreements and licensing models. Enterprise agreements allow schools to group many

existing agreements together into a single flexible agreement, at significant cost savings in overhead and management resources. Licensing models are also changing for some technology solutions, such as certain cybersecurity solutions, which can be subscription-based and supported through the cloud, rather than a single, large software/hardware purchase. These licensing models are flexible, allowing schools to place services where they need them most and to upgrade to appropriate capabilities over time. Maintenance for these cloud or software-based services are often required, and do not fit into the old definition of basic maintenance for hardware. Further, licenses for both hardware and software features are packaged together since there can be many specific features that are needed for proper network operation and security for schools. Rather than sorting through dozens of features, administrators can choose the level of features that best fits their needs. Indeed, as new, flexible software technologies are used to deploy and manage networks, the concept of a single management server and software application with network configuration files has been replaced with a comprehensive, automated and integrated network analytics capability that greatly enhances service value and reduces administrative time and resources to operate the network.

The Commission should update the eligible services list to recognize that basic maintenance of interal connections encompasses all of these models through which basic maintenance is delivered today.

C. The Commission Should Recognize That Network Security Is a Critical Component of Internal Connections

Other than firewalls, the Commission currently does not provide Category Two support for equipment and software necessary to protect the security of schools' and libraries' internal connections "in order to ensure internal connections support is targeted efficiently at the

equipment that is necessary for LANs/WLANs."[8] This forced economy is no longer necessary, however, in the current environment. For the same reason that the Category Two budgets guard against overspending on basic maintenance of internal connections, the budgets also guard against overspending on security solutions.

Today, security solutions to address cyberattacks in various forms are a necessary apect of architecting networks. For example, this year the Governor of Louisiana declared a state of emergency as a result of "severe, intentional cybersecurity breaches" in multiple school systems "that may potentially compromise other public and private entities throughout the State."[9] In response to the attack, school districts shut down their Internet access and telephone service just two weeks before fall classes began.[10] Similarly, last summer a school district in Minnesota was hit with a ransomware attack for the second time in three years.[11] Declining to pay the ransom, the school had to spend over $15,000 to restore lost data and repair damaged servers.[12]

As cyberattacks such as these are on the rise, it is imperative that connected school systems incentivize the use of effective security controls, including the ability to update, patch, and monitor systems on a 24/7 basis using cloud-based services and software technologies.

---

[8] 2014 E-Rate Order at 8918 ¶ 121.

[9] State of Louisiana, Proclamation No. 115JBE2019, "State of Emergency – Cybersecurity Incident" (July 24, 2019), http://gov.louisiana.gov/assets/EmergencyProclamations/115-JBE-2019-State-of-Emergency-Cybersecurity-Incident.pdf.

[10] *See* "Louisiana School System Takes Precautions After Cyber Attack," The Advocate (Baton Rouge) (July 31, 2019), https://www.govtech.com/education/Louisiana-School-System-Takes-Precautions-After-Cyber-Attack.html.

[11] *See* "Cloquet School District Hit By Second Ransomware Attack," Pine Journal (Aug. 17, 2018), https://www.pinejournal.com/news/4486912-cloquet-school-district-hit-second-ransomware-attack.

[12] *Id.*

Security technologies that improve safety and security enable educators to safeguard the investments they have made and are making in technology. Moreover, cybersecurity functionality today is often a part of the software on a given network component. While separate security appliances continue to play an important role (e.g., firewall servers), increasingly cybersecurity functionality is embedded in – or, built in to – network software and cloud solutions.[13] Protection against insertion of malicious software, run-time defenses, and remediation capability are examples of cybersecurity capabilities that allow for a multi-layered approach to network security, and which today are built into networking solutions. There often is no natural breaking point that would allow for treatment of network connectivity as one line item and network security as another. Network operations require security to be built into the architecture and not bolted on as an afterthought. Therefore, rather than requiring that security solutions be cost-allocated out of internal connections costs, we recommend including in internal connections support a complement of technologies that secure the network, the network's ability to access web resources, and endpoints, including:

> Identity services. These solutions provide certified identities to all users on the network, which is the basis for all access to services. Data security is based upon keeping data secure, identifying only those who should have access to that data, and allowing access only to them. Without latest generation identity services, identities can be inconsistent across the district, leading to data breaches, or identities compromised through insecure legacy systems.
>
> Policy-based enforcement. Once identities are clearly established across the school district enterprise, applications are protected by defining and enforcing policies with regard the specific users that are allowed access in specific circumstances to the application and its data. This is accomplished through adaptive and risk-based policies

[13] Cisco, Trustworthy Solutions: Built-In Security, available at https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html?dtid=osscdc000283

that are done today through software and hardware services, often through secure cloud services and maintenance support for flexibility and control.

Domain Name System security. DNS is a critical service providing access to all IP-based network services, and can be abused through a number of ways to cripple or subvert information flows. Effective protections for school DNS services are now available as cloud services, with maintenance support required for constant, rapid updates to current threat origins.

Mobile and desktop device security detection and prevention. Students, teachers, and school administrators are using mobile devices and applications more and more over time. As this happens, the threat surface exponentially increases as more and more devices are deployed, with new, sometimes unknown applications added every day. Cyber threats and attacks from inside the school occur from the lack of security inside these devices and applications. Device endpoint security software applications provide visibility to attacks across all devices in the district and allow school administrators to shut down spread of malware or ransomware quickly and sometimes automatically, before infections spread across all systems. These services are software-based applications, with subscription licensing and maintenance support.

Zero trust security model, multi-factor authentication. Today schools can strive toward a security model that verifies whether anything and everything that tries to connect to the school network, from any location, is securely challenged. One mechanism that verifies challenges is multi-factor authentication, which requires more than just a username and password to be authenticated. These security services are provided as software-based services, with the flexibility of subscription licensing and cloud maintenance support services.

With school data breaches continuing to cause not only loss of confidential data, but also bringing down operational networks for days or weeks at a time due to server or end-user device malware, school cybersecurity integrity at the network, device, and cloud level is critically important for reliable network operation and service to staff and students. As a result, the Commission should reconsider its now outmoded decision to limit network security support to firewalls and modify the definition of internal connections to include the components discussed above.

Further, the Commission should recognize that internal connections capabilities, including cybersecurity capabilities, increasingly are being provided through licensing models and enterprise agreements.[14]

A requirement to cost-allocate security services out of hardware or software purchases, whether made through traditional channels, licensing models, or enterprise agreements, results in wasted time for applicants and the Administrator, and ultimately increases the likelihood of appeals that will consume Commission resources unnecessarily. The Commission therefore should update the eligible services list for internal connections to recognize the importance of security capabilities and the models through which these capabilities are being procured today. Given the constraints imposed by applicant-specific budgets, the Commission can do so without risk of causing spikes in demand or disrupting the distribution of support among applicants.

IV. EQUIPMENT TRANSFER RULES SHOULD BE SIMPLIFIED TO REFLECT THE FIXED BUDGET APPROACH

Consistent with the proposal in the NPRM, Cisco supports easing the equipment transfer rules within school districts. This change will provide needed flexibility to school districts making decisions about best use of existing technology. Today, districts are required to make decisions as to equipment placement for a period of three years, which restricts district future choices in placing existing equipment based on the greatest need. This can cause inefficiencies and poor performing systems in certain locations when equipment transfers cannot be made to resolve issues or re-balance resources.

[14] *See supra* Section III.B.

V. CONCLUSION

Cisco urges the Commission to make the five-year Category Two budgets permanent and recognize the need for a budgetary reset for all applicants under the new rules. The Commission also should provide consistent support for much-needed basic maintenance of internal connections, including software- and cloud-based approaches that are currently prevalent. Finally, support for internal connections should include crucial support for security measures to protect schools' and libraries' supported investments in their ability to connect to the Internet.

Respectfully submitted,

CISCO SYSTEMS, INC.

By: */s/ Jeffrey A. Campbell*
Jeffrey A. Campbell
Vice President, Government Affairs
Cisco Systems, Inc.
601 Pennsylvania Avenue, NW
Washington, DC 20003
(202) 354-2920

August 16, 2019